UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
NORTHERN DIVISION

DICE CORPORATION,

Plaintiff,

v.

BOLD TECHNOLOGIES, LTD,

Defendant.

Case No. 11-CV-13578

District Judge: Hon. Thomas L. Ludington

Magistrate Judge: Hon. Mark Randon

Craig W. Horn (P34281)
Braun Kendrick Finkbeiner PLC
Attorney for Plaintiff
4301 Fashion Square Blvd.
Saginaw, MI 48603
(989) 498-2100
crahor@bkf-law.com

R. Christopher Cataldo (P39353)
David S. McDaniel (P56994)
Jaffe, Raitt, Heuer & Weiss, PC
Attorneys for Defendant
27777 Franklin Rd., Ste. 2500
Southfield, MI 48034
(248) 351-3000
ccataldo@jaffelaw.com
dmcdaniel@jaffelaw.com

Peter M. Falkenstein (P61375)
Jaffe, Raitt, Heuer & Weiss, PC
Attorneys for Defendant
201 S. Main St., Ste. 300
Ann Arbor, MI 48104
(734) 222-4776
pfalkenstein@jaffelaw.com

DEFENDANT'S MOTION FOR SUMMARY JUDGMENT

Defendant Bold Technologies, Ltd., through its undersigned counsel, moves this Court pursuant to Fed. R. Civ. P. 56 for dismissal of all counts of the Plaintiff's complaint with prejudice for the reasons set forth in the accompanying Brief, which is incorporated herein by reference.

WHEREFORE, Defendant Bold Technologies, Ltd. requests dismissal of the Plaintiff's complaint with prejudice, or the grant of such other relief pursuant to Fed. R. Civ. P. 56, to which Defendant is entitled.

Respectfully Submitted,

s/ R. Christopher Cataldo
R. Christopher Cataldo (P39353)
David S. McDaniel (P56994)
Jaffe, Raitt, Heuer & Weiss, PC
Attorneys for Defendant
27777 Franklin Rd., Ste. 2500
Southfield, MI 48034
(248) 351-3000
ccataldo@jaffelaw.com
dmcdaniel@jaffelaw.com

Dated: June 29, 2012

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN
NORTHERN DIVISION

DICE CORPORATION,

Plaintiff,

v

BOLD TECHNOLOGIES, LTD,

Defendant.

Case No. 11-CV-13578

District Judge: Hon. Thomas L. Ludington

Magistrate Judge: Hon. Mark A. Randon

Craig W. Horn (P34281)
Braun Kendrick Finkbeiner PLC
Attorney for Plaintiff
4301 Fashion Square Blvd.
Saginaw, MI 48603
(989) 498-2100
crahor@bkf-law.com

R. Christopher Cataldo (P39353)
David S. McDaniel (P56994)
Jaffe, Raitt, Heuer & Weiss, PC
Attorneys for Defendant
27777 Franklin Rd., Ste. 2500
Southfield, MI 48034
(248) 351-3000
ccataldo@jaffelaw.com
dmcdaniel@jaffelaw.com

Peter M. Falkenstein (P61375)
Jaffe, Raitt, Heuer & Weiss, PC
Attorneys for Defendant
201 S. Main St., Ste. 300
Ann Arbor, MI 48104
(734) 222-4776
pfalkenstein@jaffelaw.com

BRIEF IN SUPPORT OF DEFENDANT'S MOTION FOR SUMMARY JUDGMENT

TABLE OF CONTENTS

Pages

LIST OF CONTROLLING AUTHORITIES

Page(s)

CASES

RULES

STATUTES

STATEMENT OF ISSUES PRESENTED

I. Should the Court grant this motion under FRCP 56 and dismiss Count I of the Second Amended Complaint filed under the Michigan Uniform Trade Secret Act, MCL 450.1902 ("MUTSA") where none of the information identified in the complaint qualifies as a "trade secret" and where there is no evidence of any conduct by Defendant that would constitute "misappropriation" under MUTSA?

II. Should the Court grant this motion under FRCP 56 and dismiss Count II of the Second Amended Complaint filed under the Digital Millenium Copyright Act, 17 USC 1203 where no evidence exists that Bold circumvented any technological measure that controls access to any copyrighted work?

III. Should the Court grant this motion under FRCP 56 and dismiss Count III of the Second Amended Complaint filed for copyright infringement under 17 USC 106 where there is no evidence that Bold incorporated Dice's allegedly copyrighted software into Bold's conversion program and the conversion program does not qualify as a "derivative work" as defined in 17 USC 101?

IV. Should the Court grant this motion under FRCP 56 and dismiss Count IV of the Second Amended Complaint filed under the Computer Fraud and Abuse Act, 18 USC 1030, where there is no evidence that Bold ever accessed any "Dice Servers"?

Defendant Bold Technologies, Ltd. answers "YES" to all of the above.

I. INTRODUCTION

Defendant Bold Technologies, Ltd ("Bold") has moved this Court for dismissal of all counts of the Plaintiff's Second Amended Complaint pursuant to FRCP 56. This suit is between two software developers who both license software to alarm companies. Although the words printed on the pages of the complaint suggest that the case is about software theft and the unauthorized access to the Plaintiff's computer system, it is really about the Plaintiff's use of the complaint itself as a means to thwart competition.

In the summer of 2011, Plaintiff Dice Corporation ("Dice") was reeling from the adverse publicity surrounding the movement of its most prominent customer, ESC Central, from Dice software to Bold. To create adverse publicity against Bold, Dice filed this suit on August 16, 2011, claiming that Amy Condon, a former Dice employee who recently moved to Bold, had hacked into Dice's servers in Bay City, Michigan and Dice servers located at client sites and stolen Dice's signal processing software. To the contrary, neither Amy Condon nor anyone else at Bold has ever accessed any Dice server or customer server without permission, and Bold has never stolen any of Dice's software. The evidence below shows that at the time the suit was filed, Dice knew this. Tellingly, even though Dice knew that the allegations against Bold and Condon were untrue, it sent the complaint to its customers, urging them to review the allegations before deciding to move their business.

In November of 2011, Dice filed a Second Amended Complaint. Rather than drop the false claim that Amy Condon had hacked into Dice servers, Dice repeated this allegation verbatim, and added the equally groundless allegation that Bold had incorporated the source code from Dice's copyrighted alarm monitoring software into a Bold's extraction program, a program which performs a different function and does not incorporate any Dice computer code.

There are four counts in the Second Amended Complaint and no evidence to support any of them. As set forth below, there are no trade secrets at issue, and even if there were, there is no evidence that Bold "misappropriated" anything. Dice's claim for copyright infringement fails, as there is no evidence that Bold's extraction program incorporated or used any source code or object code from Dice's copyrighted receiver driver program. Dice's claims under the Digital Millennium Copyright Act, and the Computer Fraud and Abuse Act, fail as there is no evidence that Amy Condon, or any other Bold employee, ever accessed any Dice server, or ever accessed a customer's server without the customer's permission.

Discovery is now over. Bold respectfully submits that all of the allegations of the Second Amended Complaint should be dismissed with prejudice.

II. STATEMENT OF FACTS

1. The Parties.

Plaintiff Dice is a software developer located in Bay City, Michigan. Dice is owned 100% by its founder, Cliff Dice (Dice, Ex. A, at 6). Bold is a software development company located in Colorado. Bold is operated by one of its owners, Rod Coles (Coles Aff, Ex B). Both Bold and Dice license software to companies in the alarm industry. Amy Condon was formerly employed at Dice and worked primarily in customer service. Condon left Dice in May 2011 and began employment at Bold in June 2011 (Condon Aff, Ex C).

Bold's and Dice's customers are alarm companies, engaged monitoring incoming alarm signals from their respective subscribers, typically residences and businesses, usually for a monthly fee. When an alarm is tripped, the incoming signal is monitored by the alarm company's central station and the alarm company will then contact the police, fire, medical authorities, or take other required actions as appropriate. Both Bold and Dice license software to these alarm companies. Bold's software is licensed under the trade name "Manitou." (Coles Aff, Ex B).

Each alarm company collects significant amounts of data regarding their respective subscribers, typically stored in databases within whatever software they use. This customer data can be voluminous, as some alarm companies service several hundred thousand subscribers. All parties agree that this customer data is created by the customer, and belongs to the customer, which has the right to access and use it at any time. The data consists of names, addresses, contact information, billing information, and information regarding the type and location of alarms for each subscriber (hereinafter the "Customer Owned Data.")(Coles Aff, Ex B)(See Also Jennings, Ex F at 47).

Although Bold and Dice operate in the same market and their respective software generally performs the same function of monitoring incoming alarm signals and the ancillary functions needed by an alarm company to operate, the Bold and Dice software differ greatly in features and performance—Bold's software is state of the art whereas the Dice software is much older in design and appearance (Coles Aff, Ex B). In addition, the Bold and Dice software are very different at the technical level. Bold's Manitou software uses Windows as its operating platform and is written in the Microsoft computer language C++ and Visual Basic. Dice's software uses Thoroughbred Basic as its language and for data control and access, and uses Linux as its operating platform (Narowski Aff, Ex D). Bold has no ownership rights to Windows or any other Microsoft product, which can be licensed by the public. Similarly, Dice has no ownership rights in either Thoroughbred Basic or Linux which also can be licensed by the public (Coles Aff, Ex. B).

2. The Conversion Of An Alarm Company From One Software To Another.

Because many of the issues presented arise in the context of an alarm company switching from one software to another, it will be useful to explain that process. Generally, because an

alarm company is actively monitoring alarm signals from thousands of subscribers, the transition from one software to another must be done seamlessly to ensure that the new software is interpreting the incoming alarm signals consistent with the old software so that no alarm signals are missed or misread. The actual conversion process can take several months to complete, with additional time needed to resolve follow up issues and complete the required training of the customer's staff (Coles Aff, Ex B).

After the alarm company signs the license agreement for the new software, one of the first steps in the conversion process is the movement of the alarm company's Customer Owned Data from the databases in the old software to databases in the new software. In manuals it provides to its new customers, Dice explains that it uses any of three methods to convert Customer Owned Data from the customer's old software to the new Dice system, the second of which involves Dice copying the customer's old software and then extracting the Customer Owned Data (Ex E at 23). Dice's data conversion method #2 involves the actual copying of the customer's old software on a disk or the transmission of the old software to Dice through an electronic file transfer mechanism know as FTP (Ex E at 23). When Bold converts a Dice customer to Manitou, Bold has used an extraction program written in Thoroughbred Basic to extract the Customer Owned Data from the Dice databases and then convert the data into Manitou (Narowski Aff, Ex D).

After the Customer Owned Data has been extracted and converted to the new software, the next step is to run the customer's central station "live" on the old software with the new software running in parallel on separate servers. The customer will run the two software systems in parallel for approximately three months to ensure that the new software is accurately

monitoring the incoming signals consistent with the old system. After this, the customer will go "live" on the new software and then terminate its license for the old software. (Coles Aff, Ex B).

3. ESC Central.

ESC Central ("ESC") is an alarm company located in Birmingham, Alabama. ESC monitors alarms for approximately 400 dealers, with a total of about 50,000 subscribers (Jennings, Ex F at 6-7). ESC used Dice software from December 2001 until August 2011, a little less than 10 years (Jennings, Ex F at 10). ESC owns the servers used to run the Dice software (Ex F at 39). Kristi Jennings (formerly Harris) is ESC's part owner and operations manager (Ex F at 8). As explained below, ESC's 2011 move from Dice to Manitou gave rise to this suit.

Before its 2011 conversion to Manitou, ESC was perhaps Dice's most prominent customer. Jennings was the chairperson of the Dice users group established by Dice to better relations with its customers (Jennings, Ex F at 11). As chairperson, Jennings was liaison between Dice and its customers on a variety of issues, such as input concerning new features. As chair of the Dice users group and through daily use, Jennings became so familiar with the "ins and outs of the software and how it worked" that she gave sales demonstrations to at least 20 potential new Dice customers on the function of the Dice software (Ex F at 13-14). At Dice's request, she traveled to Dice's office to revamp its disaster recovery center (Ex F at 15-16).

Jennings was also part of the Dice "chart code committee." One piece of hardware used by alarm companies is known as a receiver, a device produced by several non-party manufacturers. If an alarm is tripped at subscriber's home or business, the alarm signal is sent to the receiver which passes the signal to the software running at the alarm company which interprets the signal and the alarm company contacts the police, fire, medical, or takes other

appropriate action. As part of this process, the receiver will label each type of signal with a code[1] as determined by the manufacturer of the respective receiver (Jennings, Ex F at 16-17). The chart code committee consisted of representatives of various Dice customers who contacted the various receiver manufacturers and gathered information on the various receiver codes for submission to Dice (Jennings, Ex F at 20). Dice then published the list of chart codes compiled by the chart code committee to each customer under the file name "ALSCHART" in the Dice software (Jennings, Ex F at 21). The codes in the ALSCHART file were not proprietary to Dice as they were a compilation of codes created by various receiver manufacturers (Jennings, Ex F at 21-22). Dice's customers had complete access to the ALSCHART file on their Dice system and the Dice customers were not restricted from accessing the information (*See* Dice customer manual, Ex G, page 3)(Jennings, Ex F at 48). The same information contained in ALSCHART could be re-created by contacting the various receiver manufacturers or from the internet (Jennings, Ex F at 55-56).

4. Dice Alienates Its Customers, Including ESC.

According to Jennings, by the summer of 2010 a mutiny was brewing between Dice and its customers (Ex F at 26). ESC and other Dice customers were having serious problems with their software that Dice refused to fix. The problems had grown so severe that it was common talk that the Dice users would soon begin looking for replacement software (Ex F at 28). Rather

[1] These alarm codes merely label the specific type of alarm signal received to allow the comparison of similar types of signals (Coles Aff, Ex B). For example, one manufacturer may assign the code "A" to burglar alarms and "B" to fire alarms. Another manufacturer may assign "B" to burglar alarms and "F" to fire alarms, etc. These alarm codes, which are really just labels, should not be confused with computer software, which consists of instructions to a computer usually described as "source code" or "object code." Source Code is the instruction to a computer written in a computer language, common examples of which are C++ and Java. Object code is the translation of the source code into a computer readable format such as binary coding. Source code is readable by humans whereas object code is readable only by computers (Narowski Aff, Ex D).

than address his customers' concerns, Cliff Dice announced a reduction of 30% of Dice's customers at a Dice users group meeting, claiming he was shrinking his company. Cliff Dice further told his customers at this meeting that anyone who did not like his direction was free to leave (Jennings, Ex F at 28-30). Dice sent at least two emails to his disgruntled customers directing them to take their business elsewhere (*See* Exhibits H and I). Jennings had no intent to move ESC off the Dice software until she received the first of these (Jennings, Ex F at 30).

As a result of the email from Dice, Jennings contacted Bold's president, Rod Coles, and asked him for information. Jennings testified that she solicited Bold in October 2010; it was not Bold who solicited ESC (Jennings, Ex F at 32-33). Jennings also obtained information from MicroKey, another Dice competitor (Ex F at 33). Even so, Jennings would have preferred that Dice just fix the problems (Ex F at 34). Jennings testified that Cliff Dice himself and two programmers came to ESC in January 2011, resulting in a "horrible experience" as this visit created a 50% chance of ESC's system crashing on a daily basis (Ex F at 34). Jennings testified that the "final straw" occurred in February 2011, when she sent a desperation email to Dice begging for help (Ex J), and made the final decision to move when Dice again ignored her plea (Jennings, Ex F at 36-37). In February 2011, Jennings contacted Chuck Speck of Bold for a quote—Bold did not solicit ESC (Ex F at 38).

5. ESC Begins Converting From Dice To Bold In April Of 2011.

ESC formally signed the license agreement with Bold in April 2011 (Jennings, Ex F at 38). The conversion of ESC's Customer Owned Data from the old Dice system to the new Bold Manitou system took place in late April to early May (Jennings, Ex F at 40). The new Manitou software was running in parallel with the old Dice software from early June until early August of 2011 (Jennings, Ex F at 40-41).

About three months after Bold converted ESC's Customer Owned Data, an event occurred in July 2011 which would later become Dice's excuse for filing this suit. In July 2011, ESC wanted to access the ALSCHART file in the Dice software running on its servers for its own use (Jennings, Ex F at 47-48). ESC was a fully licensed user of the Dice software at the time as it did not terminate its Dice license until August 2011 (Ex K). The Thoroughbred software which controls access to databases within Dice has a report writing function known as "Query" which allows users to pull data in the form of a report (Jennings, Ex F at 49-50). Dice provides a manual to its customers explaining how to use Thoroughbred Query for this purpose (Ex L).

In July 2011, an ESC employee asked Amy Condon (the former Dice employee now working for Bold), to assist her in drafting a Thoroughbred Query for several reports from the ESC servers running Dice software, one of which included ALSCHART (Condon Aff, Ex C). Condon did not log on to the ESC servers or the Dice software on this occasion. The ESC employee who made the request logged on to the ESC system using an ESC authorized password (Condon Aff, Ex C). Jennings gave permission for the use of her authorized user password for access to the ESC server on this occasion (Jennings, Ex F at 51). Condon never obtained or used any of the reports that were generated from these queries, nor were any of the resulting reports, including the ALSCHART report, provided to Bold (Condon Aff, Ex C). Bold does not use the codes in the ALSCHART file as it has its own list of alarm codes that it uses (Coles Aff, Ex B). Condon never accessed ESC's system using an administrative password (Jennings, Ex F at 50). Condon has never accessed or attempted to access any server of Dice at its Bay City office or any other location after terminating her employment there, nor has she ever accessed or attempted to access a customer's computer system without the customer's permission (Condon Aff, Ex C).

ESC went live on Manitou on August 6, 2011. In August 2011, at least one other customer besides ESC left Dice for Bold (Jennings, Ex F at 41-42). On August 8, 2011, Bold issued a press release announcing that ESC Central had upgraded its software from Dice to Bold, and foretold the movement of additional customers and employees from Dice to Bold (Ex M).

6. Dice Files False Claims Against Bold.

Seeking to blunt the sting of having the former chairperson of its user group move to Bold and to counteract the August 8 press release forewarning additional defections, Dice filed this suit on August 16, just 8 days later. In the original complaint, Dice twisted the legitimate July 2011 query run at ESC to obtain the ALSCHART file into the groundless accusation that Amy Condon had hacked into Dice servers and stolen its software. In the original complaint, Dice alleged that in July 2011 Condon had accessed Dice servers located in Bay City and accessed electronic file layouts that contained proprietary signal processing intelligence software. Dice also alleged that between July 12 and July 25, 2011, Condon also accessed "Dice Servers" located at client sites and initiated file transfers of proprietary signal processing software (*See* August Complaint, Ex N, ¶11). Based on these allegations, Dice asserted claims for trade secret violation, conversion and unjust enrichment.

The depositions of two key Dice employees, Julie Coppens and Johsua Grecko, revealed that when Dice filed the August complaint it knew that the allegations against Condon and Bold were false. Coppens testified that on August 5, 2011 she saw a picture on Facebook posted by Jennings showing the unplugging of two cables (Coppens, Ex O at 27). Using a phone access that had not been disconnected, Coppens accessed the ESC servers to see what functions were being run (Coppens, Ex O at 28). Coppens admitted that ESC owned the servers she accessed

(Ex O at 28). ESC described Dice's conduct as "illegal entry" to its servers without consent (Jennings, Ex F at 42-44) and threatened suit if Dice ever did it again (Ex P).

During this unauthorized access, Coppens saw that reports had been run using Thoroughbred Query in July 2011 which included the ALSCHART file which she believed could have been used by ESC to convert its customer data to a new software system (Coppens, Ex O at 29). Coppens printed screen shots of the Query report requests which were marked as an exhibit during her deposition (Coppens, Ex O at 37). Coppens acknowledged that ESC owned the customer data, had the right to access it, and had the right to move the customer data to a new software system (Coppens, Ex O at 29-30). Coppens testified that she could not determine who ran the Query reports on the ESC servers (Coppens, Ex O at 32-33). Coppens verified that the searches run on the ESC servers in July of 2011 were run with ESC's authorized user password (Coppens, Ex O at 35). Coppens advised Cliff Dice of the results of her investigation in August 2011 and he advised her to "fix it" so people can't query the table." (Coppens, Ex O at 35 and 53). Dice then changed its software in September 2011 to block user access to the ALSCHART file (Coppens, Ex O at 34).

Grecko is the network operations director and chief technical officer of Dice (Grecko, Ex Q at 6). Grecko is responsible for maintaining security of the Dice servers to ensure that no one can hack in from the outside (Grecko, Ex Q at 12). Grecko testified that no outside party has ever accessed the Dice system without authorization (Grecko, Ex Q at 14-16). He admitted that Dice had no evidence that Condon had ever accessed any Dice servers after she left Dice (Grecko, Ex Q at 21). Although he speculated about the possibility of an ex-employee using the password of a current employee to gain access, he had no evidence that Condon had ever done so or attempted this (Grecko, Ex Q at 22, 30-31). Grecko's investigation whether Condon had

accessed the Dice servers after she left Dice yielded no evidence (Grecko, Ex Q at 30-31). Grecko reported the results of his investigation to Cliff Dice (Grecko, Ex Q at 25-27).

Notwithstanding this investigation that yielded no evidence of any improper access or theft of software, Dice filed the complaint on August 16, 2011, knowingly asserting the false allegation that in July 2011 Condon hacked into and stole software off Dice servers in Bay City and "Dice Servers" at client sites. *See* August Complaint, Exhibit N, ¶ 10. Dice made these false claims against Bold and Condon for the purpose of stopping any further defection of Dice customers to Bold, as Dice sent a copy of the complaint to his customers, urging them to read and consider the allegations before moving their business (Ex R).

7. The Second Amended Complaint.

Dice filed its Second Amended Complaint (the "SAC") on December 5, 2011 (Ex S). The SAC repeated the same false allegations contained in the August complaint regarding Condon's alleged hacking into Dice servers in July 2011 (Ex S, ¶ 12). But the SAC included new allegations as well, alleging that Dice is the owner of software on three receiver driver programs protected by copyright which it lists (Ex S, ¶ 9).

Based on these allegations, Dice purports to plead a claim for violation of the Michigan Uniform Trade Secret Act for the alleged theft of its "signal processing intelligence" in Count I (Ex S, ¶ 14). Count II purports to plead a claim under the Digital Millennium Copyright Act, 17 USC §1203, alleging that Bold circumvented encryption on the Dice copyrighted software (Ex S, ¶ 22). In Count III, Dice alleged that Bold "incorporated Dice's copyrighted software into Bold's conversion program, and that Bold's conversion program is a "derivative work" as defined in 17 USC §101 resulting in a copyright violation (Ex S, ¶¶ 26-29). In Count IV, Dice

purported to plead a claim under the Computer Fraud and Abuse Act, 18 USC §1030, alleging again that Bold improperly accessed "Dice Servers." (Ex S, ¶¶ 32-33).

8. The New Allegations in the Second Amended Complaint.

The SAC raised two allegations not contained in the original complaint: 1) Dice's allegations regarding its copyrighted software (Ex S, ¶ 9), and the allegation that Bold's "extraction program" incorporated Dice's copyrighted software within and is a "derivative work" as defined in 17 USC §101 (Ex S, ¶¶ 26-27). The extraction program is mentioned for the first time in the SAC in Count III and the allegations regarding the extraction program are pled only with respect to Count III. (SAC, ¶¶ 26-29).

Cliff Dice admitted that his company filed for the copyright registrations referred to in the SAC after this lawsuit started (Dice, Ex A at 14). Dice has many different receiver driver programs, and Dice did not know whether ESC was using any of the three that were eventually registered for copyright (Dice, Ex A at 56). Regardless, the ALSCHART file that Dice claims was accessed in July of 2011 is not software, but a compilation of labeling codes, that is, merely a collection of codes assigned by various manufacturers to label the type of signals coming in to their respective receivers (Jennings, Ex F at55-56)(*See also* Footnote 1, *supra*). Dice conceded that its copyright did not encompass the ALSCHART table itself, only Dice's driver program (Dice, Ex A at 169).

In Count III of the SAC, Dice claims that Bold's extraction program incorporates Dice software into it and is a "derivative work" under the copyright laws (Ex S at 26-27). There is no evidence to support these allegations. Computer software can consist of either source code or object code. Source code is a collection of computer instructions written in some readable computer language, common examples being C++ and Java. Object code is the translation of

source code into a machine language of a computer such as binary coding. Source code is typically readable by humans whereas object code is readable only by computers (Narowski Aff, Ex D).

Bold employee Matt Narowski wrote the computer source code for the extraction program using information available to the public regarding Thoroughbred Basic together with his general knowledge of computer programming. Narowski did not read, review, copy, or rely upon any Dice source code or Dice object code when he wrote the extraction program. Narowski has not seen a copy of any Dice source code or object code since he left his employment at Dice in 2005. Bold's extraction program does not incorporate any of Dice's source code or object code (Narowski Aff, Ex D).

The function of the Bold extraction program is to extract the Customer Owned data from databases stored on the Linux operating platform used by the Dice software. The extraction program is only run after the customer has decided to replace its Dice software with Bold software, has signed a license agreement with Bold, and the customer wants to extract its data from the old databases where it is stored for movement into the new system. There are several other programs available that would also extract the customer owned data from these databases, such as Thoroughbred Query and other products available from Linux. The Bold extraction program differs from these methods because it converts the Customer Owned Data into a comma separated text file format which is more easily utilized by Bold to convert the Customer Owned Data into Manitou (Narowski Aff, Ex D).

The Bold extraction program and the Dice receiver driver software perform completely different functions. The Bold extraction program extracts data and converts it into a new format whereas the Dice software monitors alarm signals. The Bold extraction program is not capable

of operating an alarm company or of monitoring an alarm signal. When it performs the data extraction, the Extraction Program does not read or copy any Dice source code or object code and is not capable of doing so (Narowski Aff, Ex D). The Bold extraction program does not circumvent any security features built into the Dice software. The database files where the Customer Owned Data is stored are not subject to any Dice security feature and can be accessed by anyone with Thoroughbred Basic, which Bold licensed from that company (Narowski Aff, Ex D).

Dice has no evidence to contradict the Narowski affidavit or to support its claim that the Bold extraction program incorporates Dice object code or source code. Dice has not listed any expert witness in this case to give a comparison of the source code or object code of the respective Dice software and the Bold extraction program. Moreover, Cliff Dice admitted that his company had no evidence that the Bold extraction program copied any Dice computer code:

Q. So you've never looked at Bold's code; is that right?

A. Absolutely not.

Q. So you don't know that Bold copied Dice's source code, right?

A. No, we don't know that for a fact.

Dice Dep, Ex A at 167.

Dice's allegation that Bold incorporated Dice copyrighted software into its conversion program is as equally unfounded as Dice's allegation that Amy Condon hacked into its servers and stole its software. Discovery is now closed. All of Plaintiff's claims are groundless and properly dismissed pursuant to Federal Rule of Civil Procedure 56.

ARGUMENT

I. Standard Of Review.

Bold brings this motion pursuant to Fed. R. Civ. P. 56. A motion under Rule 56 authorizes summary judgment so that lawsuits that fail to present any genuine issue of material fact may be disposed of before trial. Summary judgment "should be rendered" if the pleadings, disclosure materials on file, and any affidavits show that there is no genuine issue as to any material fact and that the movant is entitled to judgment as a matter of law. Fed. R. Civ. P. 56(c); *Celotex Corp v. Catrett*, 477 U.S. 317, 322-23 (1986). In ruling on this motion for summary judgment, this Court must determine "whether the evidence presents a sufficient disagreement to require submission to a jury or whether it is so one-sided that one party must prevail as a matter of law." *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986).

Once the movant has met the burden of showing the absence of a genuine issue of material fact, the non-movant must come forward with specific facts showing that there is a genuine issue for trial. *Matsushita Electric Industrial Co, Ltd v. Zenith Radio Corp.*, 475 U.S. 574, 587 (1986). The adverse party however, "may not rest upon the mere allegations or denials of the adverse party's pleadings." Rather, the adverse party must introduce concrete evidence, by either affidavits, depositions, or some other evidence, setting forth specific facts showing that there is a genuine issue for trial. *Anderson*, 477 U.S. at 256; *Celotex*, 477 U.S. at 322-25. Pursuant to Fed. R. Civ. P. 56, summary judgment "should be rendered" if the pleadings, disclosure materials on file, and any affidavits show that there is no genuine issue as to any material fact and that the movant is entitled to judgment as a matter of law. Fed. R. Civ. P. 56(c); *Celotex Corp v. Catrett*, 477 U.S. 317, 322-23 (1986). "[S]ummary judgment procedure is properly regarded not as a disfavored procedural shortcut, but rather as an integral part of the

Federal Rules as a whole, which are designed to secure the just, speedy, and inexpensive determination of every action." *Celotex*, 477 U.S. at 327.

II. Count I Of The SAC Should Be Dismissed.

In Count I, Dice purports to state a claim under MUTSA, the Michigan Uniform Trade Secret Act, MCL §445.1901. In the SAC, Dice alleges that in July 2011 Condon accessed Dice servers located in Bay City and accessed electronic file layouts that contained proprietary signal processing intelligence software. Dice also alleges that between July 12, 2011 and July 25, 2011, Condon accessed Dice servers located at client sites and initiated file transfers of proprietary signal processing software (Ex S, ¶ 12). Dice then alleges that prior to its theft in July of 2011, the "signal processing intelligence software" was neither known to nor readily ascertainable to Dice's competitors (Ex S, ¶ 14). Dice claims to have restricted access to this information to its employees (Ex S, ¶ 15). Dice's sole possession of this information provided it with an allegedly competitive advantage and Bold allegedly knew that Dice's trade secrets were being acquired by Condon by improper means (Ex S, ¶¶ 16-17).

To prevail on a claim under MUTSA, Dice has the burden to establish that the information at issue qualifies as a "trade secret" ***and*** that Bold engaged in conduct that would meet the definition of "misappropriation" under MUTSA. Here, Dice cannot establish either element of the claim.

1. There Are No Trade Secrets At Issue.

To qualify for trade secret protection under MUTSA, MCL 445.1902, Dice has the burden to establish that the information at issue meets the definition of a "trade secret", defined under MUTSA as:

> [I]nformation, including a formula, pattern, compilation, program, device, method, technique, or process, that is *both* of the following:

> (i) Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use.
>
> (ii) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy. (emphasis added)

MCL §450.1902(d).

Based on the allegations in the SAC, there is no information at issue that would meet the definition of a "trade secret" under MUTSA. This case began when Julie Coppens, a Dice employee, accessed the ESC central's servers in August 2011, without ESC's consent, and saw that some unknown person had run a Thoroughbred Query in July 2011 for the ALSCHART file (*See* Statement of Facts, §6 above). Even though Dice knew that the person who ran the query did so using ESC's authorized user password on ESC's own servers, Dice simply made up the allegation that Condon had hacked into the Dice servers in Bay City Michigan and at client sites and had stolen Dice's signal processing intelligence software. (*See* SAC, Ex S, ¶ 12; *See* Statement of Facts, § 6 above).

First of all, the ALSCHART file that was the subject of the July 2011 Query is not a trade secret. This file is not software, but a compilation of codes sued by manufacturers of various receivers to label types of incoming signals (Jennings, Ex F at 16)(*See also* Footnote 1, *supra*). The ALSCHART file was not created by Dice and was not unique or proprietary to Dice as the alarm codes were collected by the Dice users group (which consisted the representatives from various Dice customers) who contacted various receiver manufacturers and collected the information (Jennings, Ex F at 20). Anyone could recreate the information in the ALSCHART file by contacting the manufacturers, or over the internet, and obtaining these labeling codes themselves (Jennings, Ex F at 55-56). The users of the Dice software were given free access to the ALSCHART file with their systems (*See* Dice Users Manual, Exhibit G, page 3); (*See also*

Jennings, Ex F at 48); (Condon Aff, Ex C). Dice restricted access to the ALSCHART file only in September of 2011 ***after*** discovering in August of 2011 that the users had free access to the file (Coppens, Ex O at 23-24 & 34-35). Thus the ALSCHART file was not created by Dice, was available from public sources, was not secret, and was not the subject of any measures to maintain its secrecy until at least September 2011 when Dice restricted access, which was after the alleged incident in July 2011 referenced in the SAC.

The ALSCHART file would not qualify for trade secret protection under MUTSA. The ALSCHART file may or may not have economic value to Dice, but even if it does that value is not "derived from not being readily ascertainable by proper means." MCL §450.1902(d). The same information can be obtained from the manufacturers of the receivers or from the internet. In addition, the information in the ALSCHART file was freely available to the Dice users on their own systems, as Dice did not restrict access to this file until September 2011, after it used its spyware to invade the ESC servers and discovered that ESC had run the Query in July seeking information contained in its own computer system. The ALSCHART file is not a trade secret under MUTSA. *Wysong v M.I. Industries*, 412 F.Supp.2d 612, 626 (E.D. Mich 2005)(information is not a trade secret if capable of being acquired without undue difficulty).

2. There Was No Misappropriation By Bold.

Even if Dice could show that the ALSCHART file were a trade secret, its MUTSA claim would fail as there was no "misappropriation" of any information by Bold. "Misappropriation", under MUTSA, is defined as either of the following:

> (i) Acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means.
>
> (ii) Disclosure or use of a trade secret of another without express or implied consent by a person who did 1 or more of the following:
>
> (A) Used improper means to acquire knowledge of the trade secret.

> (B) At the time of disclosure or use, knew or had reason to know that his or her knowledge of the trade secret was derived from or through a person who had utilized improper means to acquire it, acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use, or derived from or through a person who owed a duty to the person to maintain its secrecy or limit its use.
>
> (C) Before a material change of his or her position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.

MCL §450.1902(b).

"Improper means" is defined under MUTSA as:

> Theft, bribery, misrepresentation, breach, or inducement of a breach of a duty to maintain secrecy or espionage through electronic or other means.

MCL §450.1902(a).

Regarding the incident at issue in the SAC, Condon's role was to assist an ESC employee draft a Query for a report on information contained in ESC's own computer system, using access granted by ESC (Condon Aff, Ex C). Condon did not take or keep a copy of any report generated from the Query and did not provide a copy of any report to Bold (Condon Aff, Ex C). There no evidence that Bold even *obtained* the report regarding the ALSCHART file, let alone used "improper means" to do so as required by MUTSA to constitute misappropriation. Count I of the SAC should be dismissed. *See also R.C.Olmstead, Inc., v CU Interface, LLC.*, 657 F.Supp.2d 878, 897 (N.D.Ohio 2009); *affd* 606 F.3d 262 (6th Cir. 2010)(Trade Secret claim under Ohio's version of MUTSA properly dismissed where no evidence of acquisition by "improper means" existed.)

III. Count II Of The SAC Should Be Dismissed.

In Count II, based on the same allegations stated in paragraph 12 regarding Condon's alleged theft of Dice's computer processing intelligence software, Dice asserts a violation of the Digital Millennium Copyright Act ("DMCA"), 17 USC §1203. Dice alleges that its software is

encrypted to control access to its products (SAC, Ex S, ¶¶ 10 & 21). Dice then claims that Bold has used methods to circumvent this encryption and gain access to its software to unfairly compete (SAC, ¶¶ 22-23). There is no evidence to support this claim.

The DMCA here provides:

> No person shall circumvent a technological measure that effectively controls access to a work protected under this title. 17 USC 1201(a)(1)(A).
>
> As used in this subsection . . . to "circumvent a technological measure" means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove deactivate or impair a technological measure, without authority of the copyright owner . . .

17 USC §1201(a)(3).

The courts that have addressed claims under the DMCA have recognized that the statute "targets the circumvention of digital walls guarding copyrighted material." *Universal City Studios, Inc. v Corley*, 273 F.3d 429, 435 (2d Cir. 2001). The use of a password to access a computer system, even if the use of the password is not authorized, does not state a claim under the DMCA as there is no "circumvention" of any technological measure to access a computer system. *Ground Zero Museum Workshop, v Wilson,* 813 F. Supp.2d 678, 692 (D. Maryland 2011); *R.C. Olmstead, Inc. v CU Interface, LLC*, 657 F. Supp.2d 878, 888-89 (N. D. Ohio 2009), *affd*, 606 F.3d 262 (2010); *I.M.S. Inquiry Management Systems, Ltd. v Berkshire Information Systems*, Inc., 207 F. Supp 2d 521, 530-534 (S.D.N.Y. 2004).

There is no evidence that Bold circumvented any technological measure which controls access to any Dice copyrighted materials. The ALSCHART file that is the subject of the SAC is not part of Dice's copyrighted software—the ALSCHART file is not software, but a collection of codes from various alarm manufacturers and would not even be copyrightable. Cliff Dice admitted in his deposition that the copyright on his receiver driver software did not encompass

the ALSCHART file (Dice, Ex A at 169). The ALSCHART file is not subject to protection under the DMCA as it is not copyrighted material.

Moreover, there is no evidence that Condon ever accessed the ALSCHART file, as her role was limited to assisting an ESC employee draft a Query for information on ESC's computer system. Ms. Condon did not access the ESC system. The ESC system was accessed by an ESC employee using an ESC authorized password (*See* Condon Aff, Ex C)(*See* Jennings, Ex F at 51). Since leaving her employment at Dice, Condon has never at any time accessed, or attempted to access, any Dice server in Bay City or elsewhere (Condon Aff, Ex C). Condon has never accessed a customer's computer system without the customer's permission (Condon Aff, Ex C). Dice has not evidence to the contrary. Dice's employee, Joshua Grecko, who maintains the security of Dice system, admitted that Dice had no evidence of improper access to its computer system (Grecko, Ex Q at 30-31).

There is no possible basis for any claim against Bold based under the DMCA. No evidence exists that Condon, or any other Bold employee, ever circumvented any technological measure designed to control access to any Dice copyrighted software. The allegations in Count II are devoid of any factual basis and should be dismissed.

IV. Count III Of The SAC Should Be Dismissed.

In Count III, Dice alleges that Bold "incorporated Dice's copyrighted software into Bold's conversion program". (Ex S, ¶ 26). Dice then claims that Bold's "conversion program" is a "derivative work" as defined in 17 USC §101, and that Bold has violated Dice's copyright by creating this "derivative work" without Dice's authorization and contrary to its exclusive rights in its copyrighted software (Ex S, ¶¶ 27-29).

In *R.C. Olmstead, Inc. v CU Interface*, LLC, 606 F.3d 262 (2010), the Sixth Circuit clarified the requirements for a claim of copyright infringement involving software. Distilled to its essence, the plaintiff has the burden to prove "that he or she owns the copyrighted creation and that the defendant copied it." 202 F.3d at 274. The plaintiff may create an inference of copying by showing: 1) access to the allegedly infringed work by the defendant; and 2) a substantial similarity between the two works at issue. 202 F.3d at 274-75. Although the copyright laws give the owner of a copyright the exclusive right to create and use "derivative works based upon the copyrighted work", 17 USC §106(2), a second work cannot be a "derivative work" unless it has been substantially copied from the original. *Kohus v Mariol*, 382 F.3d 848,858 (6th Cir. 2003). As copyright protection extends only to those elements of the work that are original to the author, in all cases the plaintiff must show that the defendant copied "the constituent elements of the work that are original." *Kohus*, 382 F.3d 848, 853 (6th Cir. 2003).

Here, there is no evidence that Bold copied any component of the Dice copyrighted software, let alone any original component of the 3 Dice receiver driver programs identified in the SAC, ¶ 9. First of all, Dice has never identified any elements of its receiver driver programs that are original. Every software manufacturer has software that interprets the signal coming in from the receiver and Dice has made no showing of originality with respect to its 3 copyrighted programs (Rod Coles Aff, Ex B).

Even though Dice has made no showing of originality, there is no "substantial similarity" between any component of the copyrighted Dice receiver driver software and the Bold extraction program. To begin with, both perform very different functions. The Dice receiver driver software interprets alarm signals from receivers, whereas the Bold extraction program extracts the Customer Owned Data from a database and converts it into a format that Bold uses (Narowski

Aff, Ex D). The Bold extraction program is not capable of performing any of the functions of the Dice receiver software, such as monitoring or interpreting an alarm signal or of performing the same or any similar functions as the Dice software (Narowski Aff, Ex D).

Not only is there no similarity between the Dice receiver driver software and the Bold extraction program in terms of their function, there is no similarity between them at the source code or object code level. The source code for the extraction program was written by Bold employee, Matt Narowski, using information available to the public regarding Thoroughbred Basic software. Narowski did not read, use or rely upon any Dice computer source code or object code when he wrote the Bold extraction program, which does not incorporate or use any Dice source code or object code (Narowski Aff, Ex D). Cliff Dice admitted at his deposition that he had no information to support the claim that the bold extraction program actually incorporates Dice computer code (Dice, Ex A at 167). Dice has no expert and has performed no expert comparison of the Dice receiver driver programs and the Bold extraction program. There is absolutely no evidence or basis for Dice's claim that Bold incorporated Dice's copyrighted software in to Bold's extraction program, and that the extraction program is a "derivative work." There is no substantial similarity between the two works in question, and Dice had no basis to allege that the extraction program was a derivative work. Count III should be dismissed.

V. Count IV Of The SAC Should Be Dismissed.

Count IV purports to state a claim under the Computer Fraud and Abuse Act ("CFAA"), 18 USC §1030(e)(2). Dice claims that the "Dice Servers" accessed by Bold" are protected computers as defined in 18 USC §1030(e)(2) (Ex S, ¶ 32). Dice claims damages for Bold's alleged unauthorized access to its Bay City servers as well as the "Dice Servers" at client sites accessed by Bold (Ex S, ¶¶ 32-34).

For liability to attach under the CFAA, the defendant must "intentionally access a computer without authorization or exceed authorized access. . ." Under the CFAA "exceed authorized access means to: "access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled to obtain or alter." 18 USC §1030(e)(6). There is a split of authority regarding the scope of liability under the CFAA. Most courts have followed the narrow approach and hold that the CFAA prohibits only the improper access of computer information and does not prohibit misuse or misappropriation. *See Ajuba International v Saharia*, 2012 WL 1672713 (ED Mich 2012)(Ex T). Under the narrow approach, if the defendant accesses the plaintiff's computer with authorization the defendant does not violate the CFAA regardless of how he uses any information obtained. *Id.* Other courts have adopted a broader approach in employment cases, holding that an employee accesses a computer "without authorization" whenever the employee, without the employer's knowledge, acquires an interest adverse to his employer or is guilty of a serious breach of loyalty. *See Guest-Tek Interactive Entertainment, Inc. v Pullen*, 665 F. Supp.2d 42, 54 (D. Mass. 2009). In the recent case of *Ajuba, supra*, Judge Battani of this Court ruled that the narrow approach is the better reasoned one and the most consistent with 6th Circuit precedence. 2012 WL 1672713 at 10-12 (Ex T).

This Court does not need to even reach the question of whether to follow the narrow or the broad approach, as Dice's CFAA claim fails for an even more fundamental reason—there is no evidence that Bold "accessed a computer without authorization or exceeded authorized access" – there is no evidence that Bold ever accessed any "Dice Servers" as alleged in Count IV. Count IV purported to be based upon the SAC, ¶12, in which Dice alleged that Bold's Amy Condon hacked into Dice's servers at its Bay City office and at client sites (Ex S, ¶ 12). There is

no evidence to support this. Condon has never accessed or attempted to access any dice servers located in Bay City or elsewhere at any time after terminating her employment there (Condon Aff, Ex C). Condon has never accessed a customer server without the express permission of the customer (Condon Aff, Ex C). In the July 2011 incident referred to in the SAC, Condon did not access the ESC Servers. ESC's employee logged on to ESC's system using an ESC authorized user password (Condon Aff, Ex C). Joshua Grecko, the head of security for the Dice computer system, admitted that Dice had no evidence that anyone had ever accessed any Dice server without authorization (Grecko, Ex Q at 14-16), and no evidence that Condon at any time accessed or attempted to access any Dice server without authorization (Grecko, Ex Q at 30-31). Given the total lack of evidence supporting this claim, Count IV should be dismissed.

VI. Conclusion.

Ironically, this case did begin with a CFAA violation, but Dice was the perpetrator, not the victim. Dice's unauthorized access to ESC's servers in August 2011 would give rise to a CFAA claim by ESC against Dice should ESC decide to pursue the claim. Dice hacked into the ESC servers in August 2011 and "discovered" the legitimate Query run on ESC's own system from which it fabricated the story that Amy Condon hacked into the Dice servers and stole Dice's software when it knew those allegations were false, as Dice needed a way counteract the Bold August 8 press release (Ex M), and to convince his unhappy customers not to defect, using the complaint for that purpose (Ex R). Dice's claim that Amy Condon hacked into its Bay City servers to steal software is particularly egregious. The deposition testimony of Coppens and Grecko, two Dice employees, confirm that the complaint in this case was filed in bad faith, as Dice knew that the underlying allegations regarding Amy Condon were untrue (*See* Statement of

Facts, §6 above). In addition, Dice's claim that Bold incorporated Dice's copyrighted receiver driver software into its extraction program never had any legitimate basis in fact.

For the forgoing reasons, Bold asks that this Court dismiss all of this case under FRCP 56, or grant such other relief in Bold's favor as permitted under the Federal Rules. Bold reserves the right to file a separate motion for Rule 11 sanctions.

Respectfully Submitted,

/s/ R. Christopher Cataldo
R. Christopher Cataldo (P39353)
David S. McDaniel (P56994)
Jaffe, Raitt, Heuer & Weiss, PC
Attorneys for Defendant
27777 Franklin Rd., Ste. 2500
Southfield, MI 48034
(248) 351-3000
ccataldo@jaffelaw.com
dmcdaniel@jaffelaw.com

Dated: June 29, 2012

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
NORTHERN DIVISION

DICE CORPORATION,

Plaintiff,

v.

BOLD TECHNOLOGIES, LTD,

Defendant.

Case No. 11-CV-13578

District Judge: Hon. Thomas L. Ludington

Magistrate Judge: Hon. Mark Randon

Craig W. Horn (P34281)
Braun Kendrick Finkbeiner PLC
Attorney for Plaintiff
4301 Fashion Square Blvd.
Saginaw, MI 48603
(989) 498-2100
crahor@bkf-law.com

R. Christopher Cataldo (P39353)
David S. McDaniel (P56994)
Jaffe, Raitt, Heuer & Weiss, PC
Attorneys for Defendant
27777 Franklin Rd., Ste. 2500
Southfield, MI 48034
(248) 351-3000
ccataldo@jaffelaw.com
dmcdaniel@jaffelaw.com

Peter M. Falkenstein (P61375)
Jaffe, Raitt, Heuer & Weiss, PC
Attorneys for Defendant
201 S. Main St., Ste. 300
Ann Arbor, MI 48104
(734) 222-4776
pfalkenstein@jaffelaw.com

CERTIFICATE OF SERVICE

I hereby certify that on June 29, 2012, I electronically filed the foregoing papers with the Court using the E-File & Serve system which will send notification of such filing to the following counsel of record:

Craig W. Horn
Braun Kendrick Finkbeiner PLC
4301 Fashion Square Blvd.
Saginaw, MI 48603
crahor@bkf-law.com

s/ R. Christopher Cataldo
R. Christopher Cataldo (P39353)
Jaffe, Raitt, Heuer & Weiss, PC
Attorneys for Defendant
27777 Franklin Rd., Ste. 2500
Southfield, MI 48034
(248) 351-3000
ccataldo@jaffelaw.com